CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

June 16, 2004

Ms. Marlene H. Dortch
Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W. Room TW-A325
Washington DC 20554

Re: ***Ex Parte* Presentation**
In the Matter of Joint Petition for Rulemaking to Resolve
Various Outstanding Issues Concerning the Implementation of the
Communications Assistance for Law Enforcement Act (RM-10865)

Dear Ms. Dortch:

This is to inform you that Jerry Berman and John Morris of the Center for Democracy & Technology met on June 15, 2004 with Commissioner Jonathan Adelstein and Scott Bergmann, Legal Advisor to Commissioner Adelstein.

The purpose of this meeting was to convey the perspective of the Center for Demicracy & Technology on the policy and technical issues raised by the pending Joint Petition filed by Law Enforcement seeking, among other things, to extend CALEA to cover the Internet and Internet applications. The substantive points and concerns conveyed by CDT are detailed in the attached document, which CDT provided to meeting attendees. In addition, CDT discussed the June 16 testimony of CDT Executive Director James Dempsey before the Senate Commerce Committee, and provided copies of that testimony (attached).

Pursuant to the Commission's rules, this letter and the attached documents will be filed via the Commission's Electronic Comment Filing System for inclusion in the public record of the above-referenced proceeding.

Respectfully submitted,

/s/

John B. Morris, Jr.

cc: Commissioner Jonathan Adelstein
Scott Bergmann

Attachments: CDT CALEA Talking Points
James Dempsey Testimony

CALEA and the Internet

Center for Democracy & Technology (CDT)

DIVERSE GROUPS FROM INDUSTRY AND THE PUBLIC INTEREST COMMUNITY FILED A JOINT STATEMENT OPPOSING THE FBI PETITION

- Contrary to the text and legislative history of CALEA: CALEA covers "telecommunications common carriers," but does not cover "information services," i.e., the Internet

- Harmful to Internet innovation, security, privacy

- Unnecessary

- Signers ranged from ACLU and Electronic Frontier Foundation to Americans for Tax Reform and Free Congress Foundation and included (among others) the Computer and Communications Industry Association, the Computing Technology Industry Association, the Information Technology Association of America, and the Voice on the Net (VON) Coalition.

CALEA LEGISLATIVE HISTORY MAKES CLEAR THAT THE INTERNET IS EXCLUDED

- The House Report on CALEA stated that CALEA obligations "do not apply to information services, such as electronic mail services, or on-line services, such as Compuserve, Prodigy, America On-line or Mead Data, or Internet service providers."

- The House Report stated that "[e]arlier digital telephony proposals covered all providers of electronic communications services . . . . That broad approach was not practical. Nor was it justified to meet any law enforcement need."

- The House Report stated that "[i]t is also important from a privacy standpoint to recognize that the scope of the legislation has been greatly narrowed. The only entities required to comply with the functional requirements are telecommunications common carriers, the components of the public switched network where law enforcement agencies have always served most of their surveillance orders."

- Then-FBI Director Louis Freeh testified at a joint congressional hearing on CALEA in 1994 that a broader bill covering all communications service providers "was rejected out of hand."

- Freeh also testified that "[t]he current legislative proposal focuses on where the problems are – within the networks of common carriers. Hence, all other types of service providers (computer networks, PBX operators, etc.) have been eliminated from coverage."

- Freeh also testified that "the coverage of the legislation focused on common carriers – entities that historically have been subject to regulation. We have acknowledged, as have [congressional] subcommittees, that almost all of our electronic surveillance problems have occurred, and will continue to occur in the foreseeable future, in the networks and systems of common carriers. Therefore, this legislation does not unreasonably and unnecessarily call upon small private branch exchange (PBX) operators, pure computer networks, or private networks to alter their systems and networks."

LAW ENFORCEMENT HAS NOT PRESENTED A FACTUAL RECORD SHOWING THAT THERE IS A PROBLEM

- First round comments said that FBI had failed to demonstrate that there was any problem that needed to be solved.

- DOJ/FBI reply comments ignored those calls for evidence of problem.

- The FBI's CALEA Implementation Unit (CIU) has refused to engage in a dialogue that might reveal what problems (if any) need to be addressed. CDT -- both on its own behalf and on behalf of the larger informal working group of industry and public interest groups -- has reached out to FBI asking to meet. CDT seeks to have discussions at both a policy level and a technical level.

THREE RECENT DOCUMENTS SHOW THAT CALEA IS FUNDAMENTALLY BROKEN

- Reply Comments of the Telecommunications Industry Association (TIA), filed with the Commission on April 27, 2004:

    - Provides detailed picture of the FBI's involvement in and demands to standards organizations.

    - FBI demands that standards be developed on a "service-by-service" basis, which would be a disruptive, expensive, and never-ending process on the Internet.

    - FBI seeks to require that each new Internet service be designed to provide 100% of the "call identifying" information that exists in the circuit-switched work (even when the Internet service does not itself create or use the demanded information) *plus* any new set-up information that the service itself use

    - FBI obstructs standards organizations that do not agree to all of its demands

- "Implementation of the Communications Assistance for Law Enforcement Act by the Federal Bureau of Investigation," a report issued on April 7, 2004, by the Office of the Inspector General (OIG) of the U.S. Department of Justice, available at http://www.usdoj.gov/oig/audit/FBI/0419/final.pdf:

    - The OIG's report confirms the picture painted by the TIA filing and shows that the FBI's demands for 100% compliance has caused enormous problems within the CALEA standards setting efforts of industry.

    - The costs of CALEA for the PSTN have been much higher than Congress anticipated.

    - The OIG effectively agrees that only Congress can grant what Law Enforcement is asking the Commission to give.

- "Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications" (the "2003 Wiretap Report"), issued April 30, 2004, available at http://www.uscourts.gov/wiretap03/contents.html:

    - Out of 1,442 wiretaps authorized in 2003 for both federal and state law enforcement, a grand total of *12* (less than one percent) involved electronic wiretaps of computer communications.

    - All 12 wiretaps were successful.

    - Out of all 1,442 authorized wiretaps, the "most active" was the interception of a DSL line in Minnesota.

    - Out of the 1,442 authorized wiretaps, a single one involved the use of encryption, and in that one instance the encryption did not prevent law enforcement from obtaining the plain text of the communication.

- These documents confirm that in an effort to address a tiny fraction of the electronic interceptions to date -- all of which appear to date to have been successful -- Law Enforcement wants to impose onto the Internet a enormously disruptive and expensive burden.

LAW ENFORCEMENT *MUST ITSELF* DEVELOP THE CAPABILITIES THAT LAW ENFORCEMENT WANTS TO IMPOSE ON INDUSTRY.

- FBI's focus on services and service providers ignores the fact that sophisticated criminals can cut out third parties service providers and communicate directly or with in-house developed techniques.

- Third party services developed overseas (as more and more will be if the Joint Petition is granted) can be used to wholly avoid CALEA requirements.

- Even domestic third party services can be encapsulated within other communications protocols to evade the demanded interception capabilities of industry.

- Unless law enforcement intends to cede the field to criminals, far and away the most effective technical approach to Internet interception is for law enforcement to develop the ability to understand Internet communications (instead of simply demanding that such communications be translated into circuit-switched terms).